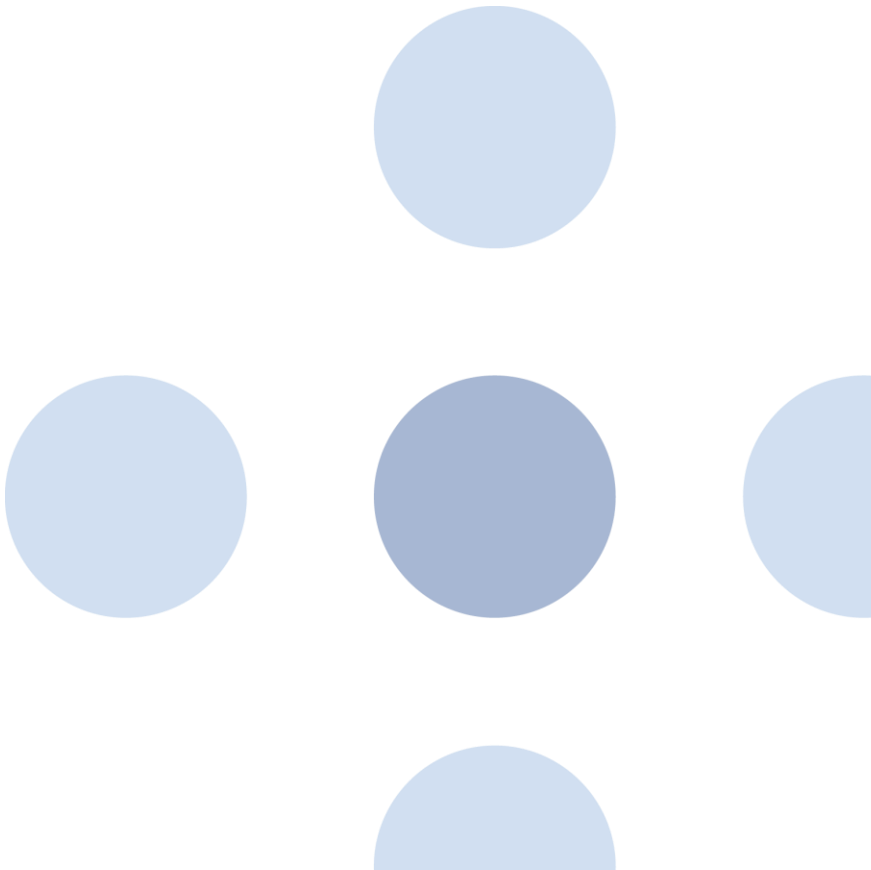
Regional fagplan IKT-beredskap

Helse Midt-Norge

Endringshistorikk

Versjon	Endret av	Dato
1.1	Godkjent RLIP	27.11.2024
1.0	Godkjent RLIP	12.05.2022
0.9	Hemit HF	11.03.2022



Innhold

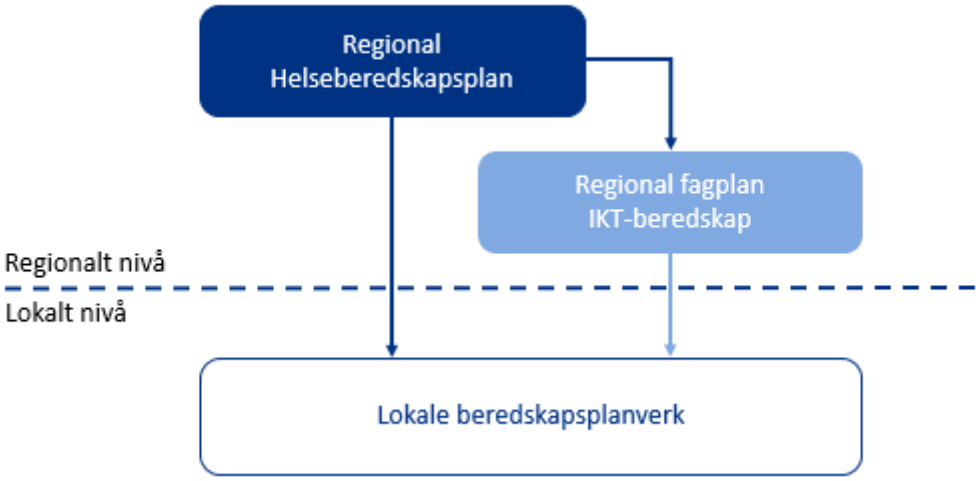
1 Innledning

1.1 Formål, omfang og avgrensninger

Regional fagplan for IKT-beredskap beskriver ansvar, sammenhenger, kommunikasjonslinjer og krav til IKT-beredskap mellom helseforetakene, Hemit HF og Helse Midt-Norge RHF.

Fagplan for IKT-beredskap er en del av Regional helseberedskapsplan for Helse Midt-Norge. Beredskapsplanverket består av en regional fagplan for IKT-beredskap (dette dokumentet) og lokale beredskapsplaner i den enkelte virksomhet. Hensikten med planverket er å sette virksomhetene i Helse Midt-Norge i stand til å håndtere uventede og uønskede hendelser som kan komme til å inntreffe, eller omfatter brudd på tilgjengelighet, konfidensialitet og/eller integritet for informasjon og IKT-systemer.

Sammenhengen mellom Regional helseberedskapsplan, Regional fagplan for IKT-beredskap og lokale planverk er illustrert i figur 1.



Figur 1 Beredskapsplanverk

Regional fagplan for IKT-beredskap gjelder for Helse Midt-Norge og omfatter all digital behandling av informasjon i virksomhetene i Helse Midt-Norge.

Krav til beredskap knyttet til IKT-tjenestene Hemit leverer er beskrevet i «Avtale om IT-tjenester» 1 som inngås mellom virksomheten og Hemit. Avtaler mellom sykehusforetakene og Hemit gjør rede for samarbeid og ansvar relatert til ivaretakelse av Medisinsk teknisk utstyr.

[1] http://virksomhetsportal.helsemn.no/omrader/hemit/kundeportal/sla/default.aspx

Fagplanen inneholder ikke spesielle krav til interne og eksterne IKT-tjenesteleverandører. Slike krav forutsettes håndtert i «Avtale om IT-tjenester» (Hemit) eller tjenesteavtaler (Helseplattformen AS og andre leverandører).

1.2 Ansvar for beredskapsplanen

Eierdirektør i Helse Midt-Norge RHF er ansvarlig for Regional fagplan for IKT-beredskap. Eierdirektør i samarbeid med beredskap (RHF) skal sikre at regionale og lokale planverk innen IKT-området er samordnet.

Regional fagplan for IKT-beredskap skal revideres i henhold til krav gitt i Regional helseberedskapsplan for Helse Midt-Norge og i regionalt styringssystem for informasjonssikkerhet og personvern i Helse Midt-Norge.

1.3 Kilder til krav og føringer for IKT-beredskap

Kilder til Nasjonale, regionale og lokale krav og føringer for IKT-beredskap er listet i tabellen nedenfor. Den enkelte virksomhet er i tillegg ansvarlig for å ha oversikt over de krav og føringer de omfattes av.

Tabell 1 Nasjonale, regionale og lokale krav og føringer

Kilde	Krav og føringer
Lov om helsemessig og sosial beredskap (Helseberedskapsloven)	Gjelder blant annet for den offentlige helse- og omsorgstjeneste. Loven stiller krav til at regionale helseforetak og sykehus omfattet av loven, skal utarbeide en beredskapsplan for de helse- og omsorgstjenester de tilbyr.
Forskrift om krav til beredskapsplanlegging og beredskapsarbeid mv. etter lov om helsemessig og sosial beredskap.	Virksomhetene skal utføre beredskapsplanlegging som gjør dem i stand til å tilby nødvendige tjenester under krig og ved kriser og katastrofer i fredstid i samsvar med lov om helsemessig og sosial beredskap § 1-1. Forskriften stiller krav til arbeidet med beredskapsplanlegging.
Lov om spesialisthelsetjenesten (§2.1 b)	Stiller krav om at RHFet utarbeider en beredskapsplan i tråd med helseberedskapsloven
Norm for informasjonssikkerhet (Normen)	Normens kapittel 5.9 stiller krav om at virksomheten skal sørge for at nødvendige helse- og personopplysninger er tilgjengelige, kartlegge konsekvensen av bortfall, klassifisering og prioritering av systemer. Med utgangspunkt i klassifiseringen av informasjonssystemene skal virksomheten etablere nødrutiner: - Alternativ drift uten bruk av informasjonssystemene - Alternativ drift med delvis støtte fra informasjonssystemene

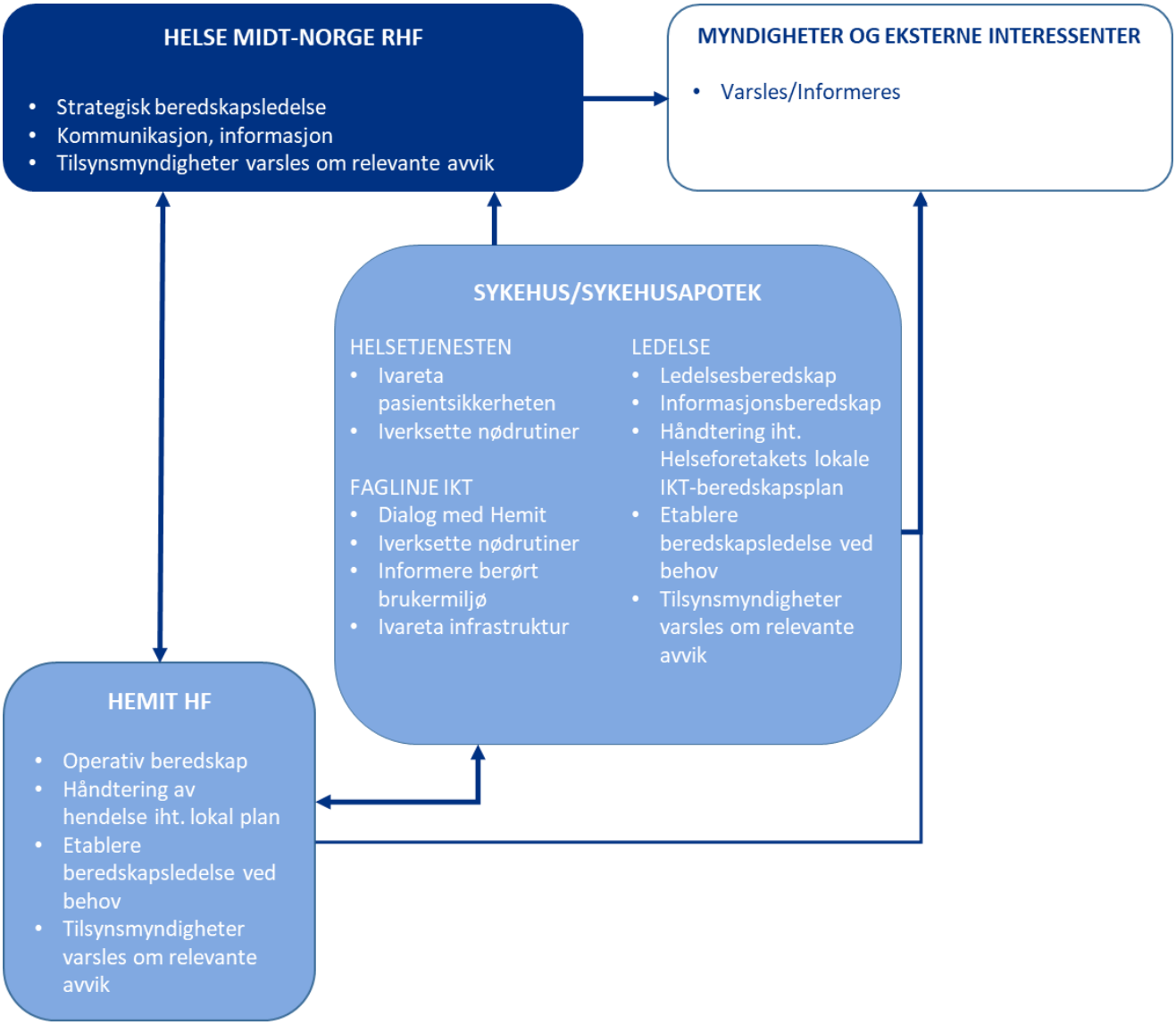
	Nødrutinene skal øves på, testes, revideres og oppdateres minst en gang i året.
Regional helseberedskapsplan for Helse Midt-Norge	Stiller krav om at det skal utarbeides en regional fagplan for IKT-beredskap. Det stilles også krav innenfor andre områder, aktiviteter og faser som er relevant for beredskapsplanlegging og håndtering.
Avtale om IT-tjenester	Regulerer forholdet mellom helseforetakene/virksomhetene og Hemit HF som tjenesteleverandør, herunder krav om SLA, varsling mm.
Databehandleravtale	Avtale mellom dataansvarlig og databehandler som regulerer databehandlers behandling av personopplysninger på vegne av dataansvarlig
Regionalt styringssystem for informasjonssikkerhet og personvern	Beskriver blant annet roller og ansvar mellom virksomhetene knyttet til informasjonssikkerhet og personvern.
NSM grunnprinspper	Kapittel 4 i NSM Grunnprinsipper beskriver spesielt prinsipper for håndtering og gjenoppretting under/etter en hendelse.
Sikkerhetsloven	Beskriver blant krav om varslingsplikt. Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata
Klareringsforskriften	Beskriver krav til klarering av personell ved håndtering av gradert informasjon (viktig at blir ivaretatt, også under en krise/hendelse).
Regional samhandlingsavtale mellom Hemit og MTA/ATA	Beskriver ansvarsfordelingen mellom Hemit og MTA/ATA (nå i versjon 0.9, men skal nå være klar for signering av respektive avdelingssjefer).

2 Beredskapsnivå

I Helse Midt-Norge er det definert fire beredskapsnivå. De ulike nivåene er beskrevet i Regional helseberedskapsplan kapittel 3.7.2.

3 Organisering, roller og ansvarsområder

Regional helseberedskapsplan Helse Midt-Norge beskriver overordnet organisering og ansvarsfordeling. Figur 2 viser en overordnet beskrivelse av ansvar i en beredskapssituasjon. Pilene viser varslingslinjer.



Figur 2 Overordnet organisering, roller og ansvar (ikke uttømmende) IKT-beredskap Helse Midt-Norge.

Varsling skjer i henhold til Regional helseberedskapsplan, og de gjeldende prosedyrer for varsling hos de enkelte virksomheter.

Alle virksomhetene som omfattes av Regional fagplan for IKT-beredskap skal varsle øvrige virksomheter om IKT-hendelser som vil kunne påvirke den regionale beredskapen eller andre virksomheter sin beredskap.

Ved IKT-hendelser der respons er tidskritisk for å begrense skadeomfanget (for eksempel ved et dataangrep) kan Hemit være nødt til å stenge ned berørte tjenester med umiddelbar virkning. I slike tilfeller skal Hemit uten opphold varsle berørte foretak/virksomheter om nedstengningen og forventet nedetid. Dette reguleres i Avtale om IT-tjenester.

Berørte foretak/virksomheter som er brukere av IKT-tjenester skal ha gjort seg kjent med hvilke konsekvenser bortfall av berørte tjenester vil kunne ha for pasientbehandling og andre kritiske driftsfunksjoner, og ha etablert tilstrekkelig beredskap.

3.1 Alle virksomheter

Håndtering og varsling av IKT-hendelser skal være i tråd med det enkelte foretaks prosedyrer og planverk.
Den enkelte virksomhet, HF og RHF har ansvar for å informere Hemit om hvem som skal være varslingsmottakere i egen virksomhet.

Den enkelte virksomhet skal ha beredskapsplaner for å ivareta konfidensialitet, integritet og tilgjengelighet for hele eller deler av infrastrukturen, for IKT-systemer som anses som kritiske av virksomheten, samt for informasjonen som behandles i disse.

3.1.1 Særskilt for Hemit

Den operative beredskapen av IKT-hendelser håndteres i henhold til etablert prosess i Hemit (Incident Management). Prosessen har til hensikt å sikre at Hemit klarer å ivareta de forpliktelser som følger av «Avtale om IT-tjenester». Incident-prosessen skal sørge for at hendelser som påfører eller kan komme til å påføre redusert tjenestekvalitet enten avverges eller rettes/løses så raskt som mulig. Avhengig av type hendelse forsterkes arbeidet med relevante interne fagteam og eksterne samarbeidspartnere. Hemit etablerer beredskapsledelse som støtte til operativ beredskapshåndtering, enten som følge av en krise/katastrofe i Hemit eller ved et helseforetak, eller en alvorlig IKT-hendelse som er eskalert etter ordinære rutiner i Hemit i henhold til avtale med virksomhetene. Hemit har en beredskapsplan som iverksettes ved alvorlige eller potensielt alvorlige IKT-hendelser.

«Avtale om IT-tjenester», vedlegg 2, gjør rede for avtalt varsling av ulike typer hendelser og varslingskanaler fra Hemit til virksomhetene.

Når det etableres beredskapsledelse i Hemit på grunn av en eskalert hendelse sendes situasjonsrapport i HelseCIM fra Hemit. Avhengig av situasjonen vurderes telefonisk kontakt.

3.1.2 Særskilt for Helse Midt-Norge RHF

Helse Midt-Norge RHF har et regionalt ansvar som trer inn ved virksomhetsovergripende IKT-hendelser. I slike situasjoner skal Helse Midt-Norge RHF sørge for koordinering, ekstern kommunikasjon og informasjon.

3.2 Informasjonsdeling og situasjonsrapporter Helse-CIM

Formidling av informasjon om aktuelle hendelser gis gjennom situasjonsrapporter sendt via HelseCIM. De enkelte virksomheter er ansvarlig for å sikre at riktig personell/roller mottar informasjonen.

Noen situasjoner kan være av en slik art at ikke all informasjon kan deles gjennom åpne kanaler. Dette kan skyldes at deler av informasjonen er gradert iht. sikkerhetsloven eller at hendelsen er under etterforskning og som gjør at informasjonen i enkelte tilfeller må begrenses.

3.3 Prioritering av gjenoppretting

Ansvaret for å gjenopprette IKT-tjenester på en hensiktsmessig måte tilligger Hemit. Ved gjenoppretting kan det måtte gjøres prioriteringer mellom ulike tjenester og ulike helseforetak/virksomheter, på bakgrunn av avtalt tjenestenivå for de ulike tjenester og gjennom dialog mellom Hemit HF og berørte helseforetak/virksomheter.

Avbøtende tiltak som gjøres ved IKT-hendelser kan i noen tilfeller medføre at tjenester som ikke er direkte berørt av hendelsen påvirkes.

4 Overordnede krav og retningslinjer for IKT-beredskap i HMN

Krav til IKT Beredskap for virksomhetskontinuitet	
4.1	Foretakene skal sikre at IKT-beredskapsplaner, inkludert reaksjons- og gjenopprettingsprosedyrer (som beskriver hvordan organisasjonen planlegger å håndtere forstyrrelser i IKT-tjenester); 1) er utarbeidet, dokumentert og implementert i foretaket 2) regelmessig blir evaluert, forbedret og oppdatert gjennom øvelser og tester; 3) er godkjent av ledelsen i foretakene Foretakene skal sikre at det foreligger en tilfredsstillende organisasjonsstruktur med personell med nødvendig ansvar, myndighet og kompetanse for å forberede seg på, redusere og reagere på en hendelse.
4.2	Foretakene skal utarbeide strategier for å vedlikeholde og beholde relevant IKT kompetanse og ferdigheter for medarbeidere og eksterne nøkkelressurser.
4.3	Foretakene skal utarbeide strategier for å redusere konsekvensene av at de ordinære IKT fasiliteter ikke lenger er tilgjengelige som følge av hendelser eller katastrofer. Strategiene skal baseres på identifisert risiko og kravene til å sikre tjenester som understøtter grunnleggende nasjonale funksjoner.
4.4	IKT-beredskapsprosesser og prosedyrer skal etableres og dokumenteres slik at innholdet er tydelig og på et detaljnivå som gjør det mulig for kompetente ressurser å gjennomføre disse uten unødvendige forsinkelser eller uklarheter.

4.5	Prosessen og/eller prosedyren for iverksetting av en IKT beredskapsplan skal være klart definert og dokumentert. Prosessen skal sikre at relevante planer eller delplaner kan iverksettes på kortes mulig tid, enten i forkant av en potensiellforstyrrende hendelse eller umiddelbart etter at en hendelse har inntruffet.
4.6	Foretakene skal identifisere og dokumentere eksterne avhengigheter som støtter IKT tjenestene og ta forholdsmessige steg for å sikre at kritisk utstyr og tjenester kan leveres av deres leverandører innenfor forhåndsbestemte og avtalte tidsrammer
4.7	Foretakene skal inkludere IKT- beredskapskrav og krav til virksomhetskontinuitet i Avtale om IT-tjenester med Hemit HF, samt for eventuelle øvrige leverandører og tjeneste-tilbydere. Kontrakter og avtaler skal inkludere referanse til hver parts forpliktelser, avtalte servicenivåer, respons på større hendelser, kostnadsfordelinger, trenings- og øvelsesfrekvens og korrigerende tiltak.
4.8	Foretakene skal gjennomføre årlige øvelser, ikke kun for formålet å gjenopprette IKT tjenester, men også å teste tjenestenes beskyttelse og robusthet for å fastslå om: - en tjeneste kan beskyttes, opprettholdes og/eller gjenopprettes uavhengig av hendelsens alvorlighetsgrad; - IKT beredskapen bidrar til å minimere konsekvensen for foretaket; og om - prosedyrene for gjenoppretting til «business as usual» virker slik de skal. Når en øvelse er gjennomført skal funnene gjennomgås og følges opp umiddelbart.
4.9	Foretakene skal sikre at det finnes tilfredsstillende vaktordninger og varslingsrutiner for håndtering av hendelser.
4.10	Foretakene skal basert på vurderingen av kritiske tjenester og systemer utarbeide og vedlikeholde en liste over prioriterte informasjonssystemer.

5 Krav til håndtering av Informasjonssikkerhetshendelser

5.1	Foretakene skal planlegge og forberede for håndtering av informasjons-sikkerhetshendelser i samsvar med etablerte rutiner for avvik og hendelseshåndtering i foretaket. Der det er relevant skal foretaket sørge for nødvendig bistand fra og samhandling med tjenesteleverandør i håndtering av informasjonssikkerhetshendelser i henhold til gjeldene avtale om IT-tjenester med tilhørende databehandleravtale.
5.2	Foretakene skal vurdere informasjonssikkerhetsavvik og avgjøre om disse skal kategoriseres som informasjonssikkerhetshendelser. Det skal minimum eksistere en egen kategori for informasjonssikkerhets- og personvernavvik i foretakets avvikssystem (EQS).
5.3	Kunnskap tilegnet som følge av informasjonssikkerhetshendelser skal brukes til å styrke og forbedre sikkerhetstiltakene for informasjonssikkerhet. Foretakene skal etablere prosedyrer for å kvantifisere og overvåke typer av informasjonssikkerhetshendelser, volumet og kostnader ved slike hendelser.

5.4	Alle sikkerhetshendelser, eller begrunnet mistanke om slike, som medfører stor risiko for den registrerte skal meldes til tilsynsmyndighetene.

Krav ved innsamling av mulige bevis	
5.5	Foretakene skal sørge for at identifisering, innsamling, anskaffelse og bevaring av mulige bevis, knyttet til informasjonssikkerhetshendelser, blir gjennomført med avtalt støtte fra tjenesteleverandør der det er relevant. , Det skal være mulig å vise at: a) dokumentasjon er fullstendig og ikke manipulert på noen måte; b) kopier av mulige elektroniske bevis sannsynligvis er identiske med originalene; c) alle informasjonssystemer som det er samlet inn mulige bevis fra, fungerte som de skulle på det tidspunktet da disse ble registrert. Dette for å sikre korrekt håndtering av mulige bevis som underlag i en eventuell rettsak eller i etterforskning.
5.6	Etablerte prosedyrer skal følges ved håndtering av mulige bevis knyttet til informasjonssikkerhetshendelser som skal brukes i forbindelse med disiplinære eller rettslige skritt. For å gjøre det så sannsynlig som mulig at bevisene tillates ført, skal det tas hensyn til kravene som stilles i de relevante jurisdiksjonene.

Krav til informasjonssikkerhet ved forstyrrelser	
5.7	Foretakene skal planlegge hvordan informasjonssikkerheten skal holdes på et hensiktsmessig nivå under forstyrrelser.
5.8	Foretakene skal fastslå sine krav til tilpasning av sikkerhetstiltak for informasjonssikkerhet under en forstyrrelse. Krav til informasjonssikkerhet skal inkluderes i prosessene for styring av virksomhetskontinuitet i foretakene.
5.9	Planer og prosesser skal utvikles, implementeres, testes, gjennomgås og evalueres for å opprettholde eller gjenopprette sikkerheten til informasjon i kritiske virksomhetsprosesser under/etter en forstyrrelse. Informasjonssikkerheten skal gjenopprettes til ønsket nivå og innenfor de nødvendige tidsrammene. Det skal finnes kompenserende sikkerhetstiltak for informasjonssikkerhet som ikke kan opprettholdes under en forstyrrelse.